CLAIMS:

What is claimed is:

1. A communication system for communicating securely encrypted messages, comprising:

i. a resource-constrained client;

ii. a gateway server possessing high computational power capable of doing fast and dynamic encryption-related computations when requested by the client and returning the result to the client;

iii. an application server communicating encrypted messages with the client; and

iv. a communication network connecting the client, the gateway server, and the application server.

2. The communication system as in claim 1, wherein the communication network is a wireless communication network.

3. The communication system as in claim 2, wherein the gateway server is a wireless gateway server.

4. The communication system as in claim 2, wherein the client is a mobile device.

5. The communication system as in claim 1, wherein the encrypted messages are encoded using public-key cryptography.

6. The communication system as in claim 5, wherein the public-key cryptography is achieved using RSA algorithm.

7. The communication system as in claim 1, wherein the client further comprises means for storing and generating the encryption key, generating random numbers and doing modular multiplication.

8. The communication system as in claim 7, wherein the random numbers are generated for scrambling the encryption key and the original message as well as decomposing the encryption key.

9. The communication system as in claim 8, wherein the scrambled and decomposed encryption key and the scrambled original message are sent from the client to the gateway server.

10. The communication system as in claim 7, wherein the modular multiplication is performed based on the result returned by the gateway server.

11. The communication system as in claim 1, wherein the encryption-related computations performed by the gateway server are integer exponentiation.

12. A method for encrypting a message using a client-server model, comprising the steps of:

i. the client generates random numbers;

ii. the client uses the random numbers to scramble both the encryption key and the original message as well as decompose the encryption key;

iii. the client sends the scrambled and decomposed encryption key and the scrambled message to the server;

iv. the server computes the exponentiation of the scrambled message being raised to the power of each decomposed scrambled encryption key;

v. the server sends the computation results to the client; and

vi. the client extracts the encryption result using a modular multiplication of the results returned by the sever.

13. The method as in claim 12, wherein the client is a mobile device.

14. The method as in claim 12, wherein the server is a wireless gateway server.

15. A two-iteration client-server encryption method for protecting encrypted messages from attacks made by un-trusted server, comprising the steps of:

i. the client generates multiple sets of random numbers;

ii. the client uses each set of random numbers to scramble both the encryption key and the original message as well as decompose the encryption key;

iii. the client sends each set of scrambled and decomposed encryption key and the scrambled message to the server;

iv. the server computes the exponentiation of each set of the scrambled message being raised to the power of each decomposed scrambled encryption key in the same set;

v. the server sends the computation results to the client;

vi. the client extracts the encrypted message for each set using a modular multiplication of the results returned by the sever;

vii. the client feeds the encrypted messages once more to the server and the server performs the exponentiation one more time; and

viii. the client derives the encrypted messages one more time and verifies if each set returns the same encrypted message.

16. The method as in claim 15, wherein the number of sets of random numbers is three.

17. The method as in claim 15, wherein the client is a mobile device.

18. The method as in claim 15, wherein the server is a wireless gateway server.